Cobalt Strike стал главным кибероружием против правительственных структур региона.

Китайская хакерская группа Sharp Panda, известная своими кампаниями кибершпионажа, начала атаковать правительственные организации в Африке и Карибском бассейне. Об этом сообщили специалисты из Check Point Software Technologies Ltd. – это компания, специализирующаяся на разработке и поставке продуктов и решений в области кибербезопасности для защиты компьютерных сетей, серверов и мобильных устройств от различных видов киберугроз. Она является одним из лидеров в отрасли кибербезопасности.
 Компания предлагает решения для защиты от различных угроз, таких как вредоносные программы, хакерские атаки, кибершпионаж, атаки на приложения и многое другое." data-html="true" data-original-title="Check Point" >Check Point в своём недавнем отчёте.

В рамках кампании используется вредоносное ПО Cobalt Strike's Beacon (маяк Cobalt Strike) — это компонент программного обеспечения, который является частью инструмента Cobalt Strike, известного как фреймворк для тестирования на проникновение и пентестинга. Beacon используется в кибератаках и имитирует агента внедрённого в скомпрометированную сеть или систему.

 Маяк Cobalt Strike представляет собой задачу в системе жертвы, которая обеспечивает C2-канал для злоумышленников. Он обеспечивает связь между атакующим и скомпрометированной сетью, позволяя злоумышленникам получать доступ к системе, управлять ею и выполнять различные действия, включая сбор информации, перемещение по сети, выполнение вредоносных операций и установку дополнительных инструментов.

 Beacon обладает различными функциями, которые позволяют злоумышленникам обходить системы обнаружения и предотвращения вторжений. Он может использовать шифрование и обходить обнаружение в реальном времени, позволяя атакующим длительное время оставаться незамеченными." data-html="true" data-original-title="Beacon" >Beacon, являющееся частью фреймворка Cobalt Strike представляет собой законный фреймворк для проведения тестов на проникновение, позволяющий доставить на компьютер жертвы полезную нагрузку и управлять ею. Злоумышленники же могут использовать Cobalt Strike в реальных атаках на целевые системы, эффективно совмещая фреймворк с другими инструментами." data-html="true" data-original-title="Cobalt Strike" >Cobalt Strike, которое предоставляет функции для удалённого управления заражёнными системами и исполнения команд. Использование данного инструментария позволяет минимизировать использование кастомных инструментов и сократить риск их обнаружения. По мнению экспертов Check Point, такой подход свидетельствует о глубоком понимании целей атак.

Sharp Panda, также известная как Sharp Dragon, была впервые обнаружена в июне 2021 года, когда атаковала правительство одной из стран в Юго-Восточной Азии с использованием вредоносной программы VictoryDLL. В последующих атаках хакеры использовали модульный фреймворк Soul, позволяющий получать дополнительные компоненты с серверов, контролируемых злоумышленниками, для продвинутого сбора информации.

Исследования показывают, что разработка Soul началась в октябре 2017 года. Этот бэкдор включает функции, заимствованные из Gh0st RAT и других общедоступных инструментов, часто используемых китайскими киберпреступниками.

В июне 2023 года группа атаковала высокопоставленных чиновников из стран G20, что свидетельствует о продолжающейся нацеленности на правительственные структуры для сбора информации. Важным элементом операций Sharp Panda является эксплуатация уязвимостей нулевого дня, таких как CVE-2023-0669, для проникновения в инфраструктуру и использования её в качестве C2-серверов.

Недавние атаки на правительства Африки и Карибского бассейна демонстрируют расширение целей для атак. Злоумышленники используют взломанные аккаунты электронной почты высокопоставленных лиц из Юго-Восточной Азии для рассылки фишинговых писем с вредоносными вложениями, использующими инструмент Royal Road для распространения загрузчика «5.t». Этот загрузчик осуществляет разведку и запускает Cobalt Strike Beacon, что позволяет хакерам точечно собирать информацию о целевых системах.

Использование Cobalt Strike не только снижает риск обнаружения кастомных инструментов, но и указывает на «усовершенствованный подход к оценке целей», как отмечает Check Point. Так, в последнее время хакеры также начали использовать исполняемые файлы, замаскированные под документы, для повышения шанса заражения, что является свидетельством постоянного совершенствования их тактики.

Стратегическое расширение деятельности Sharp Dragon на Африку и Карибский бассейн отражает стремление китайских киберпреступников усилить свое присутствие и влияние в этих регионах.

Хакерские группировки, подобные Sharp Panda, постоянно совершенствуют свои методы, адаптируя тактики и используя новейшие инструменты для проникновения в правительственные структуры различных стран. Их деятельность выходит за рамки

отдельных регионов, свидетельствуя о стремлении к расширению влияния и сбору конфиденциальной информации в глобальных масштабах.

Подобная вредоносная активность подчёркивает необходимость повышения кибербезопасности и укрепления международного сотрудничества в борьбе с киберпреступностью для защиты важнейших государственных структур и данных.